Magic Cubes and Secret Sharing Schemes (Algebras, logics, languages and related areas)

AUTHOR(S):

Adachi, Tomoko; Lu, Xiao-Nan

数理解析研究所講究録 第2096巻 2018年 115-118

Magic Cubes and Secret Sharing Schemes

Tomoko Adachi*, Xiao-Nan Lu**
* Department of Information Sciences, Toho University
** Department of Industrial Administration, Tokyo University of Science

1. Introduction

A secret sharing scheme in cryptography is developed for a set of participants to share secrets. The first and the most famous scheme in various secret sharing schemes, is a (t, w)-threshold scheme which was proposed by Shamir [4] in 1979. It is a method of sharing a secret value K among a finite set $\mathcal{P} = \{P_1, P_2, \cdots, P_w\}$ of w participants in such a way that any t participants can reconstruct K but no group of $t-1$ or fewer participants can reconstruct K. Each piece of information of K distributed to each participant is called a *shadow*.

A Latin square of order n is an $n \times n$ array in which n distinct symbols are arranged so that each symbol occurs in each row and column. Secret sharing schemes using Latin squares have been investigated, for instance, Cooper's scheme [1] and Stones' scheme [5]. Both schemes make use of partial Latin squares. Cooper's scheme use critical sets of Latin squares. Stones' scheme use Latin square autotopisms.

A magic square of order n is an arrangement of n^2 integers $1, 2, \cdots, n^2$ into an $n \times n$ square with the property that the sums of each row, each column, and each of the main diagonals are the same. It is known that a magic square of order n can be constructed if n is an integer for which there is a pair of orthogonal diagonal Latin squares of order n. More generally, a magic hypercube of order n and dimension t is an arrangement of n^t integers $1, 2, \cdots, n^t$ into an $n \times n \times \cdots \times n$ (t times) array with the property that the sums in each 1-dimensional subarray and each of the main diagonals are the same. Lu and Adachi [3] introduced a construction and protocol of secret sharing schemes using magic hypercubes.

We call a magic hypercube with dimension three a magic cube. In order to clarify the main ideas of using magic hypercubes for secret sharing schemes, in this paper, we introduce the secret sharing schemes using magic cubes.

2. Critical sets of Latin squares

We refer to [1] and [2] for more details on the related contents in this section.

First, we define a partial Latin square and a critical set. A *partial Latin square* of order n is an $n \times n$ array with entries chosen from the set $\{1, 2, \cdots, n\}$ in such

a way that no element occurs twice or more in any row or column. A *critical set* in a Latin square L of order n is a set $C = \{(i, j; k) \mid i, j, k \in \{1, 2, \cdots, n\}\}$ such that

(i) L is the only Latin square of order n which has symbol k in cell (i, j) for each $(i, j; k) \in C$, and

(ii) no proper subset of C has property (i).

A critical set is called *minimal* if it is a critical set of smallest possible cardinality for L.

For example, a Latin square of order 5 is given on the right as follows. A minimal critical set $C = \{(1, 1; 1), (2, 5; 3), (3, 5; 4), (4, 2; 3), (4, 3; 5), (5, 1; 5), (5, 3; 2)\}$ for this Latin square L is given on the left.

$$C = \begin{bmatrix} 1 & * & * & * & * \\ * & * & * & * & 3 \\ * & * & * & * & 4 \\ * & 3 & 5 & * & * \\ 5 & * & 2 & * & * \end{bmatrix}, \quad L = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \\ 3 & 5 & 1 & 2 & 4 \\ 4 & 3 & 5 & 1 & 2 \\ 5 & 4 & 2 & 3 & 1 \end{bmatrix}.$$

Now, we describe a secret sharing scheme using a critical set. The secret key K is taken to be a Latin square L of order n. Here, n is allowed to be public, although L is kept private. The shadows in the secret are based on a partial Latin square $\mathcal{S} = \left\{ \bigcup_i C_i \mid C_i \text{ is a critical set in } L \right\}$. For each $(i, j; k) \in \mathcal{S}$, the shadow $(i, j; k)$ is distributed privately to a participant. The number of critical sets we used is depend on the size of the Latin square and the number of participants in the secret sharing scheme. The access structure is defined to be the set $\Gamma = \{B \mid B \subset \mathcal{S} \text{ and } B \supset \mathcal{C} \text{ where } C \text{ is some critical set in } L\}$.

3. Secret sharing schemes using magic cubes

A cube of order n is *of type* ℓ $(1 \leq \ell \leq 2)$, if in each $(3 - \ell)$-dimensional subarray, each symbols occurs in the same frequency. In what follows, all the cubes we considered are of type 2 without special mention. Hence, each 2-dimensional subarray (square) forms a Latin square. For any cube, there are four main diagonals. If each symbols occurs exactly once in any of the main diagonals, the cube is said to be *diagonal*.

Moreover, three cubes of order n are said to be mutually 3-dimensionally *orthogonal* (simply, orthogonal, in the following), if when superimposed, each possible triple of symbols occurs exactly once.

We denote the element in the cell (i, j, k) of a magic cube M of order n by $M(i, j, k)$. For given three mutually orthogonal diagonal cube LC_i $(i = 1, 2, 3)$, a

magic cube can be obtained as follows:

$$M(i,j,k) = LC_1(i,j,k) \times n^2 + LC_2(i,j,k) \times n + LC_3(i,j,k) + 1 \qquad (*)$$

If n is odd or doubly even, that is $n \equiv 0, 1, 3 \pmod 4$, the existence and constructions of three mutually orthogonal diagonal LC_i $(i = 1, 2, 3)$ are known from the results in [3].

Hence, we can construct a $(3, 3)$-threshold scheme in which we consider a magic cube M as a secret key K and the corresponding three cubes LC_i $(i = 1, 2, 3)$ as shadows. Moreover, we decompose each cube LC_i into three Latin squares $L_{i,j}$ $(j = 1, 2, 3)$. Then, we can construct a $(3, 3)$-threshold scheme in which we consider each cube LC_i as a secret key K and the Latin squares $L_{i,j}$ $(i, j = 1, 2, 3)$ as shadows. Next, we use Cooper's scheme or Stones' scheme to each Latin square $L_{i,j}$. Therefore, we obtain a three-stage secret sharing scheme using a magic cube.

The protocol of our scheme is as follows:

(1) *Preparation:* We choose three mutually orthogonal diagonal cubes LC_i $(i = 1, 2, 3)$ of order n. A magic cube M of order n can be constructed from LC_i by $(*)$. The number n is made public, although the magic cube M is kept secret and taken to be the secret key K.

(2) *The first stage of distribution:* The shadows in the first stage of our scheme are the cubes LC_i $(i = 1, 2, 3)$. We define the shadow set $\mathcal{S}^{(1)} = \{LC_1, LC_2, LC_3\}$. Each shadow $LC_i \in \mathcal{S}^{(1)}$ is distributed privately to a participant. This stage is the distribution of a $(3, 3)$-threshold scheme. This stage is the first stage of our scheme.

(3) *The second stage of distribution:* We decompose each cube LC_i to three Latin squares L_{i,i_1}, for $i_1 = 1, 2, 3$. Then, we can construct a $(3, 3)$-threshold scheme in which we consider each cube LC_i as the second secret key K' and Latin squares L_{i,i_1} as shadows. We define the second stage shadow set $\mathcal{S}_i^{(2)} = \{L_{i,1}, L_{i,2}, L_{i,3}\}$. This is the second stage of our scheme.

(4) *The final stage of distribution:* Now we have nine Latin squares, namely L_{i,i_1} with $i, i_1 \in \{1, 2, 3\}$. We consider each Latin square L_{i,i_1} as the third secret key, and define a shadow set $\mathcal{S}_{i,i_1}^{(3)}$ from L_{i,i_1}, by using a critical set or an autotopism. For each element in $\mathcal{S}_{i,i_1}^{(3)}$, the shadow is distributed privately to a participant. This stage is based on the distribution of Cooper's scheme or Stones' scheme. This is the third stage of our scheme.

(5) *The first stage of reconstruction:* When a group of participants whose shadows of $\mathcal{S}_{i,i_1}^{(3)}$ constitute a critical set or an autotopism come together, they are

able to reconstruct the Latin square L_{i,i_1}. This stage is the reconstruction of Cooper's scheme or Stones' scheme.

(6) *From the second stage of reconstruction:* When three participants whose have shadows the Latin squares L_{i,i_1} of $\mathcal{S}_i^{(2)}$ come together, they are able to reconstruct the cube LC_i. This stage is the reconstruction of a $(3,3)$-threshold scheme.

(7) *The final stage of reconstruction:* When three participants whose have shadows the cubes LC_i $(i = 1, 2, 3)$ of $\mathcal{S}^{(1)}$ come together, they are able to reconstruct the magic square M and hence the secret key K. This stage is the reconstruction of a $(3,3)$-threshold scheme.

Acknowledgment

The authors would like to acknowledge the support from Initiative for Realizing Diversity in the Research Environment.

References

[1] J. Cooper, D. Donovan, and J. Seberry (1994); Secret sharing schemes arising from latin squares, *Bull. Inst. Combin. Appl.*, Vol. 12 (1994), pp. 33–43.

[2] C. F. Laywine and G. L. Mullen (1998); *Discrete Mathematics Using Latin Squares*, John Weiley & Sons, INC.

[3] X. N. Lu and T. Adachi; Secret sharing schemes using magic hypercubes, manuscript submitted for publication.

[4] A. Shamir (1979); How to share a secret, *Comm. ACM*, Vol. 22, No. 11, pp. 612–613.

[5] R. J. Stones, M. Su, X. Liu, G. Wang and S. Lin (2016); A Latin square autotopism secret sharing scheme, *Des. Codes Cryptogr.*, Vol. 80, No. 3, pp. 635–650.

[6] M. Trenkler (2000); A construction of magic cubes, *Math. Gaz.*, Vol. 84, No. 499, pp. 36–41.